CI-Group Vendor Policy

Purpose

The purpose of this policy is to set forth the guidelines that should be followed to maintain the security of the organization's information systems and data when CI-Group enters into any arrangement with a third-party supplier/vendor as well as to identify elements of managing vendors, due diligence, risk assessments as well as contract management.

Scope

The scope of this policy covers CI-Group 's relationship with business partners, suppliers, or third-party vendors (collectively referred to as ‘vendors’ or ‘third parties’) including any third-party access to information, IT assets, IT infrastructure and facilities of CI-Group and/or its client information.

Policy

Managing Outsourcing Risks

CI-Group utilizes a significant amount of vendors to carry out business operations. As such, CI-Group breaks their vendors into 2 categories:

1. Information Security Vendors
    a. These vendors assist with business operations and may have access to CI-Group and CI-Group customer data, in accordance with contracts, to assist with data processing
2. Supplier vendors
    a. These vendors assist with CI-Group’s fulfillment services to the customers they serve

Requirements for All Vendors

Not all vendors have access to CI-Group’s sensitive data, however, all vendors must comply with the following requirements:

- Business continuity procedures are in place to ensure operations are able to be recovered
- SLAs are defined and enforced
- Vendors agree to and sign CI-Group’s Human Rights Policy
- Vendors agree to and sign CI-Group’s Terms of Service documentation, or similar

contractual language of service details and terms
- All Purchase Order requirements must be fulfilled and acknowledged by vendors that do not have contractual agreements executed

This includes all information security and fulfillment vendors utilized to carry out CI-Group business operations.

Additional Requirements for Information Security Vendors

Prior to outsourcing any CI-Group ’s processes or services to a third party/vendor or allowing third-party access to the organization's information or systems, the risks involved must be clearly identified and documented. A review of third-party risks along with mitigation strategies or whether the risks are acceptable should be performed by management prior to engaging with high-risk vendors. Vendors that have access to any sensitive CI-Group or CI-Group customer data are considered high-risk vendors.

Note that vendors that do not have access to CI-Group information or systems may also be analyzed based on standards similar to those listed below, however, are only required to be analyzed after, as no access to CI-Group information systems would be obtained.

To ensure that our information is protected when handled or managed by our third parties, we consider the following security risk areas:

- The third party has implemented proper separation of duties, role-based access, and least-privilege access for all personnel (if applicable)
- Ongoing monitoring of the network and infrastructure is in place (if applicable)
- The third party provides applicable incident information to CI-Group
- Confidential or Sensitive data is encrypted in transit and at rest
- The vendor agrees to and complies with the 4 requirements for all vendors listed above.

In the event that a vendor can demonstrate that they maintain a current ISO 27001 certification, an unqualified SOC 2 Type 2 report, or equivalent reputable certification then the third party will be considered to meet the minimum requirements. Vendors who do not have either of these documents may be required to complete an information security questionnaire for CI-Group. The response to these questionnaires should be reviewed to determine if the risk associated with engaging the vendor is acceptable.

Note: The above is only applicable for high-risk vendors. Vendors that have access to any sensitive CI-Group or CI-Group customer data are considered high-risk vendors.

Contracts

Third-party relationships must be managed by contracts (supplier agreements). These contracts that include the exchange of confidential data must require confidentiality and non-disclosure agreements (NDA) to be executed by the vendor and shall identify applicable security policies

and procedures to which the vendor is subjected, where applicable.

Contracts should have standard wording, where there is not a standard MSA or license agreement. They must clearly identify security reporting requirements that stipulate that the vendor is responsible for maintaining the security of confidential data, under their control. In the event of a breach of the security of the CI-Group 's confidential data, the vendor is responsible for notifying CI-Group regarding incident details, recovery and remediation.

Third-party access to CI-Group information shall be granted only after authorization and signing the applicable agreements/contracts.

Access Provisioning

In the event that a vendor requires access to CI-Group systems and/or data, an access request must be made following the standard access request process. Access requests for vendors must, at a minimum, include:

1) A documented access request from the vendor's CI-Group manager

2) Documentation regarding why the vendor needs the access and for how long

3) A documented approval from an executive management member to provision the access

Furthermore, it is required that access shall only be granted to vendors once they have completed the requirements outlined above.

Oversight and Monitoring

Third parties shall be re-evaluated for security risks to the organization on a periodic basis through a formal risk assessment process. Vendors handling critical data/functions may be evaluated annually. The results of such periodic assessments shall be considered during service/contract renewals.

Termination of Service

Upon termination of vendor services, the owner of the third-party relationship shall:

- Revoke the vendor's access to CI-Group information systems
- Ensure that information stored or processed by the vendor is deleted in a timely manner
- Obtain a data deletion confirmation from the vendor
- Log the termination of the service